Asian Journal of Applied Science and Technology (AJAST)
Volume 10, Issue 3, Pages 95-105, July-September 2026

The Evolution of Dark Web Marketplaces: Operational Structures, Ecosystem Resilience, and Implications for the Global Illicit Economy

Bello Abubakar Bayu[1,2], Suleiman Sa'ad[3], Iliyasu Adamu[4] & Anagu Emmanuel John[1,5,*]

[1]*Department of Information Technology, Faculty of Computing, Modibbo Adama University, Yola, Adamawa State, Nigeria.*
[2]*Department of Computer Science, Federal University of Technology, Babura, Jigawa State, Nigeria.*
[3]*Department of Cybersecurity, Faculty of Computing, Modibbo Adama University, Yola, Adamawa State, Nigeria.*
[4]*Department of Software Engineering, Faculty of Computing, Modibbo Adama University, Yola, Adamawa State, Nigeria.*
[5]*Department of Information Systems, Federal University Wukari, Taraba State, Nigeria.*
Corresponding Author Email: anague@fuwukari.edu.ng[*]

DOI: https://doi.org/10.38177/ajast.2026.10305

Copyright © 2026 Bello Abubakar Bayu et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Article Received: 25 May 2026 *Article Accepted: 28 July 2026* *Article Published: 17 August 2026*

ABSTRACT

Today, dark web marketplaces (DWM) are extremely sophisticated digital communities that facilitate transnational criminal activities using anonymity networks, cryptocurrencies and decentralised management. Existing analyses of DWM anonymity infrastructure, financial systems, trust mechanisms, or enforcement operations have focused on them as separate facets, and even the most similar analyses of ecosystem survival from an existing resilience literature approach the topic from a single perspective network structure and/or enforcement dynamics instead of considering the ecosystem as the result of multi-layered, interacting technical, governance, financial, and institutional components. If one does not exist, then there is no explanation for marketplace resiliency being found across dimensions, nor for coordinated intervention to be most effective. This study fills this gap by undertaking a structured integrative literature review and proposing the Five-Layer Dark Web Marketplace Resilience and Disruption Framework. The results confirm that marketplace resilience is a property that emerges from the marketplace ecosystem: many marketplaces reopen fast after enforcement efforts, as vendors relocate, reputation is portable, decentralised financial systems come into existence, and communities continue even if the marketplace is closed. This is significant because it moves the discussion from a one-layer disruption to a multi-layer disruption, where the disruption problem is solved through multi-layer intervention, combined with blockchain intelligence, international regulatory cooperation, financial monitoring and long-term network monitoring.

Keywords: Dark Web Marketplaces; Cybercrime; Cybersecurity; Cryptocurrency; Blockchain Analytics; Marketplace Resilience; Platform Governance; Illicit Digital Economy.

1.0. Introduction

Digital technologies have revolutionized global commerce through enhanced connectivity, accessibility and efficiency. The same technology has also allowed for more sophisticated cybercrime techniques, including the rise of dark web marketplaces (DWMs). DWMs operate mainly using anonymity networks like Tor, and cryptocurrency payment systems, which allows for the trans-border sale of illegal goods and services without revealing the name and location of buyers, vendors and administrators. Unlike traditional criminal operations, these platforms provide technological anonymity and commercial features like vendor ratings, escrow services, dispute resolution and reputation systems, allowing anonymous users to build trust and maintain enduring trading relationships without formal legal protection (Christin, 2013; Aldridge & Décary-Hétu, 2016; ElBahrawy et al., 2020; Nadini et al., 2022).

As the DWMs continue to evolve, there have been significant interests in their implications for cybercrime, financial crime, drug trafficking, fraud, and global security in the fields of research, policy and law enforcement. Initial research has focused on the rise of Silk Road and proved the potential for anonymity networks and Bitcoin to create a scalable digital marketplace for illegal online commerce (Christin, 2013; Aldridge & Décary-Hétu, 2014). Recent studies reveal that current DWMs are intricate socio-technical systems, emphasizing sophisticated security measures, reputation portability, multi-platform migration, blockchain-powered financial transactions, and flexible

governance models to facilitate swift market recovery after enforcement actions (dos Reis et al., 2024; Décary-Hétu & Giommoni, 2017; ElBahrawy et al., 2020; Europol, 2026). The increasing number of such indicators shows that the resilience of the marketplace is not solely the result of technological anonymity: it is the result of the presence of technical, organisational, financial and social mechanisms on interconnected digital networks.

Despite these developments, there are still significant gaps in the literature. Previous research focused on specific components of DWMs such as trust and reputation systems, cryptocurrency transactions, enforcement, blockchain analysis, or platform security, and typically adopted a largely independent analysis of dimensions. As a result, little concept has developed regarding how these mechanisms operate together to create the long-term resilience of ecosystems in times of market disturbance. In addition, recent developments, such as privacy enhancing cryptocurrencies, decentralised trading relationships, sophisticated marketplace security measures and international regulatory reactions have increased the complexity of DWMs' operations, but few review studies include those developments in a single framework of analysis. Therefore, policy makers and researchers remain without a unified conceptual model of how the interdependencies between marketplace resilience and the potential for sustainable disruption exist and what is most likely to be successful.

There has been some previous work that has been successful in tackling certain aspects of this problem. A single marketplace is much less effective at withstanding investigations by law enforcement than is the dark net market ecosystem as a whole, as Bradley (2019) has shown empirically, and ElBahrawy et al. (2020) have quantified that buyers and vendors shift distribution between coexisting marketplaces after an investigator closes one of them. The literatures reviewed above, however, do not account for the interactions among layers – they focus on one layer of resilience without modelling the interdependencies among the layers – and neither does either of these two studies. This is significant because it leaves open the practical question of where a coordinated intervention should focus its effort and why single-layer interventions have not been effective or successful in the past. This study begins to fill this gap by first conducting a structured integrative literature review to synthesize the latest institutional and scholarly evidence from 2008 to 2026, and second by introducing a Five-Layer Dark Web Marketplace Resilience and Disruption Framework, to our knowledge, the first model to view anonymity infrastructure, platform governance, network continuity, financial adaptability, and institutional response as one interconnected resilience system, rather than as distinct research fields. The framework highlights the systemic failure of single-layer disruption strategies, by making the interdependencies explicit, and suggests what a truly coordinated, multi-layer strategy would require addressing.

2.0. Methodology

The review was done using peer-reviewed journal articles, conference proceedings, institutional reports and key technical documents published between 2008 and 2026. The scholarly literature was accessed from well-known databases and publisher platforms such as ScienceDirect's, SpringerLink, Nature Portfolio's, ACM Digital Library, PLOS, PubMed Central, Crossref-indexed journals, and university repositories. The following organisations were chosen as sources of institutional evidence because they have authoritative publications related to cybercrime investigations, virtual asset regulation, and important dark web enforcement operations, respectively: Europol, the

European Union Drugs Agency (EUDA), the Financial Action Task Force (FATF), and the U.S. Department of Justice. When it came to the basics and resources that were essential to understanding the development of the dark web marketplaces, they were retained.

2.1. Research Design

The current study used the structured integrative literature review and thematic synthesis methods to examine how dark web marketplaces developed, operated, built resilience, and how they have implications for policy. Given the research problem that crosses various disciplines (cybersecurity, criminology, platform governance, blockchain technology, financial regulation, law enforcement) the integrative review design was chosen. The integrative approach was used to go beyond mere aggregation of homogeneous empirical work and included empirical work and conceptual, technical and policy documents in order to provide an overall picture of marketplace resilience. The conceptual integration aspect was therefore emphasized in the review, and not the statistical meta-analysis or estimation of effect size.

2.2. Procedure

The list of keywords above was arrived at by conducting a systematic search on the Academic Web search engines and searching on the publishers' databases. Highly relevant studies were also identified from reference lists, to find foundation studies that are not already known.

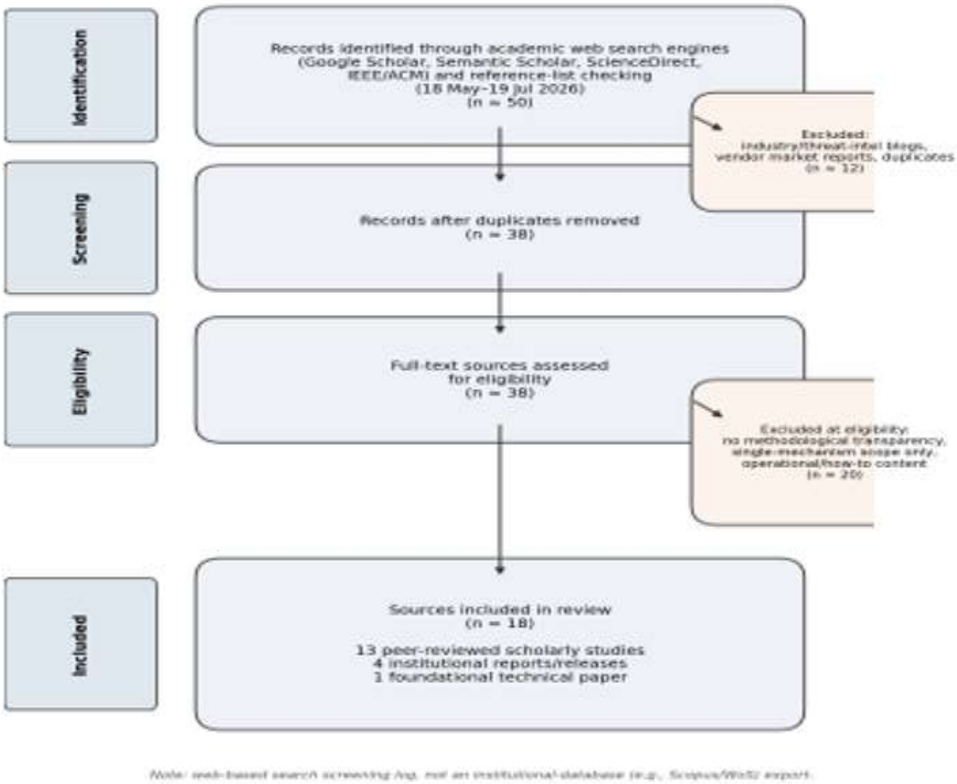
Identification
Records identified through academic web search engines (Google Scholar, Semantic Scholar, ScienceDirect, IEEE/ACM) and reference-list checking (18 May–19 Jul 2026) (n = 50)
Excluded: industry/threat-intel blogs, vendor market reports, duplicates (n = 12)
Screening
Records after duplicates removed (n = 38)
Eligibility
Full-text sources assessed for eligibility (n = 38)
Excluded at eligibility: no methodological transparency, single-mechanism scope only, operational/how-to content (n = 20)
Included
Sources included in review (n = 18)
13 peer-reviewed scholarly studies
4 institutional reports/releases
1 foundational technical paper

Figure 1. Search and screening log for this review.

The following constituted the sources accepted: (i) empirical evidence relating to the market place, virtual asset users, virtual asset vendors, virtual asset transactions or security mechanisms; (ii) publications and research on the

subject of trust, governance, resilience, migration, or cryptocurrency infrastructure; (iii) reports on major law enforcement operations; or (iv) internationally recognised guidance on virtual assets from the regulatory authorities. Content was not included if methodological transparency was not included or was not published, if it was sensationalized (newspaper articles or anonymous statistics), or if it included operational advice on how to use illegal marketplaces. Figure 1 shows the search and screening log for this review that was performed on academic web search engines (Google Scholar, Semantic Scholar, ScienceDirect, IEEE/ACM) instead of a single export from an institutional database. Unlike past narrative reviews of the resilience of dark web marketplace, evidence for each of the five layers below was not being assembled ad hoc, but rather was chosen based on pre-specified inclusion criteria, so that the framework in Figure 2 is not simply an opinion piece, but rather is based on documented evidence.

2.3. Data Analysis

They extracted data using a standardised framework, which included the publication information, source of data, methodology, main findings and reported limitations of each study. Evidence was then coded into the following 5 analytical themes: (1) anonymity and access infrastructure, (2) platform governance and trust, (3) network continuity, (4) financial adaptability, and (5) external institutional response. Themes from different studies were analyzed and compared to find common themes, commonalities, and conflicting evidence. This Five-Layer Dark Web Marketplace Resilience and Disruption Framework was created by integrating the interplay of interactions between these themes, allowing for a holistic understanding of how these technological, organisational, financial, and institutional elements collectively shape.

Table 1. Summary of included sources mapped to the five analytical themes.

Source	Year	Type	Method/Approach	Primary theme(s)
Nakamoto	2008	Foundational technical paper	Protocol specification	Financial adaptability
Christin	2013	Peer-reviewed (conf.)	Large-scale marketplace measurement	Anonymity & access infrastructure
Aldridge & Décary-Hétu	2014	Peer-reviewed (working paper)	Case study analysis	Anonymity & access infrastructure
Aldridge & Décary-Hétu	2016	Peer-reviewed journal	Cryptomarket data analysis	Platform governance & trust
Bradley	2019	Doctoral thesis	Mixed-methods ecosystem analysis	Network continuity; Institutional response
Ladegaard	2019	Peer-reviewed journal	Longitudinal case analysis	Network continuity
Tzanetakis et al.	2016	Peer-reviewed journal	Qualitative interviews	Platform governance & trust
Décary-Hétu & Giommoni	2017	Peer-reviewed journal	Longitudinal transaction analysis	Network continuity
Duxbury & Haynie	2018	Peer-reviewed journal	Network topology analysis	Platform governance & trust; Network continuity

ElBahrawy et al.	2020	Peer-reviewed journal	Large-scale network analysis	Network continuity
Bracci et al.	2022	Peer-reviewed journal	Marketplace listing analysis	Institutional response
Nadini et al.	2022	Peer-reviewed journal	Network science / graph analysis	Financial adaptability; Network continuity
Scharnowski	2024	Peer-reviewed journal	Panel regression (Kraken exchange data)	Financial adaptability
dos Reis et al.	2024	Peer-reviewed journal	Bitcoin transaction network analysis	Network continuity; Financial adaptability
Europol (IOCTA)	2017	Institutional report	Threat assessment	Institutional response
Europol (IOCTA)	2026	Institutional report	Threat assessment	Institutional response
FATF	2021	Institutional guidance	Regulatory guidance	Financial adaptability; Institutional response
FATF	2026	Institutional guidance	Regulatory guidance	Financial adaptability; Institutional response

3.0. Results and Discussion

3.1. Anonymity and Access Infrastructure

Dark web marketplaces have grown from solitary anonymous trading websites to highly flexible, multi-layered, and interconnected anonymous online marketplaces. Early cryptomarkets, especially Silk Road, illustrated the potentials of creating a functioning online marketplace for illicit commerce through anonymity networks, cryptocurrency payments, reputation systems, and escrow services (Christin, 2013; Aldridge & Décary-Hétu, 2014). These access technologies were later adapted and improved by the other marketplaces, with the implementation of extra security measures such as invitation-only registration and mirror domains to further safeguard against infiltration and takedown (Aldridge & Décary-Hétu, 2016; ElBahrawy et al., 2020; Nadini et al., 2022).

These successive layers of anonymity infrastructure are the results of the ability of the marketplace operators to learn from past disruptions and strengthen technical defenses. As the architecture of the markets has evolved, the number of languages has increased, and the communication systems have become more secure, the process of infiltration and de-anonymisation of blockchain has become increasingly difficult, while blockchain analytics have been continually improving their ability in tracing pseudonymous transactions (dos Reis et al., 2024; ElBahrawy et al., 2020). The ongoing tech arms race suggests anonymity infrastructure serves as a foundation upon which the other dimensions of marketplace resiliency (governance, network, financial, institutional) are layered.

3.2. Trust and Governance in Anonymous Markets

Even in the absence of a legal structure for enforcement, the key element of the operation of dark web marketplaces is trust. Anonymity is achieved through private governance systems such as reputation scores, vendor ratings, verified transactions, escrow services, dispute resolution processes, and community forums. These mechanisms foster continued marketplace engagement and lower the perceived transaction risk, leading to long-term marketplace involvement (Aldridge & Décary-Hétu, 2016; Tzanetakis et al., 2016; Duxbury & Haynie, 2018).

Some evidence shows that not all trust signals are equal in their contribution to marketplace stability. The cost of these signals (such as reputation, transaction history and vendor experience) demands continuous investment and are therefore less easily controlled. Cheap signals, like convincing product descriptions or nice branding names, on the other hand, can be easily duplicated with relatively little effort and potentially not signal vendor credibility. This distinction is one reason why the old vendors continue to gain customers' trust after the marketplaces get disrupted, while the new ones have more doubts.

These findings build on earlier conceptions of trust as a resilience mechanism, as well as a potential vulnerability, within the marketplace. Trust systems enable anonymous trade, but can be used to draw out recognisable patterns that can be of assistance in intelligence and targeted law-enforcement actions. This makes governance structures at the same time more stable and robust and more conducive to strategic disruption in the marketplace.

3.3. Network Continuity

Recent evidence highlights continuity in the lifecycle of marketplaces, rather than what was previously known, which mainly focused on the lifecycle of individual marketplaces. More broadly, large-scale network analyses reveal that vendors and buyers regularly engage in multihoming; when one market is shut down, participants move to other markets in existence, but not to extinction (ElBahrawy et al., 2020; dos Reis et al., 2024). This trend is confirmed by the results of longitudinal studies of enforcement actions: transactions and the number of vendors usually drops significantly shortly after the marketplaces are seized, only to rise again in the following months as displaced vendors rebuild on other platforms (Décary-Hétu & Giommoni, 2017; Ladegaard, 2019).

The platform-centric approach to resilience has given way to an ecosystem-centric approach, meaning marketplace continuity relies on a resilient social and transactional network more than on the single survival of a website. Portable reputational capital, buyer relationships, and the standard operating procedures of vendors bring to them when they move, reduce recovery time and minimize the long-term impact of single-platform enforcement actions (Duxbury & Haynie, 2018; Nadini et al., 2022). Therefore, a more comprehensive approach to disruption should be aimed at the wider marketplaces system of interdependent vendors and buyers rather than merely at specific takedowns of marketplaces.

3.4. Financial Adaptability

Cryptocurrencies are the backbone of dark web marketplaces, facilitating international and anonymous transactions without relying on any central authority. Bitcoin was crucial to the genesis of the first cryptomarkets, due to its ability to do so in two ways: it limited reliance on traditional bank systems, and it offered a transparent blockchain that enabled analysis of the transactions. Further research has shown that blockchain analytics can provide insights into transaction networks, user migration, and connections between key market actors, further establishing cryptocurrency's role as an operational tool and investigative tool for blockchain analytics (Nakamoto, 2008; ElBahrawy et al., 2020; Nadini et al., 2022; dos Reis et al., 2024).

But the financial world has become much more complex, with the use of privacy coins, cryptocurrency mixers, chain hopping and decentralised exchange (DEX) systems. The innovations make attribution difficult and make

traditional blockchain traceability less effective, and empirical evidence shows that even without significantly affecting blockchain prices, dark web traffic volume can be measured as a correlation to the volume of trading in privacy-coins on secondary marketplaces (Scharnowski, 2024). To promote financial oversight, regulatory bodies have therefore placed an increased focus on financial risks faced by VASPs, and on bolstering international cooperation and customer due diligence (FATF, 2021, 2026).

Financial disruption is best achieved when technical blockchain analysis, regulatory enforcement and international cooperation are all part of the mix. For this reason, cryptocurrency should be considered not just as a facilitating technology for criminal activity, but also as a tool to facilitate financial intelligence for long-term investigations of organised cybercrime networks.

3.5. Institutional Response

The fifth layer of marketplace resilience is provided by law enforcement and regulatory bodiesthe external forces to which the first four layers respond. The Europol's Internet Organised Crime Threat Assessment (IOCTA) reporting highlights the increase in coordinated international takedown operations over the last ten years as well as the use of blockchain analytics and the establishment of cross-border data-sharing agreements between the 2017 and 2026 assessments (Europol, 2017, 2026). These operations have repeatedly been shown to be able to take over market infrastructure, uncover administrators and temporarily interrupt the trading process, while ecosystem-level continuity (Section 3.3) prevents its enduring impact.

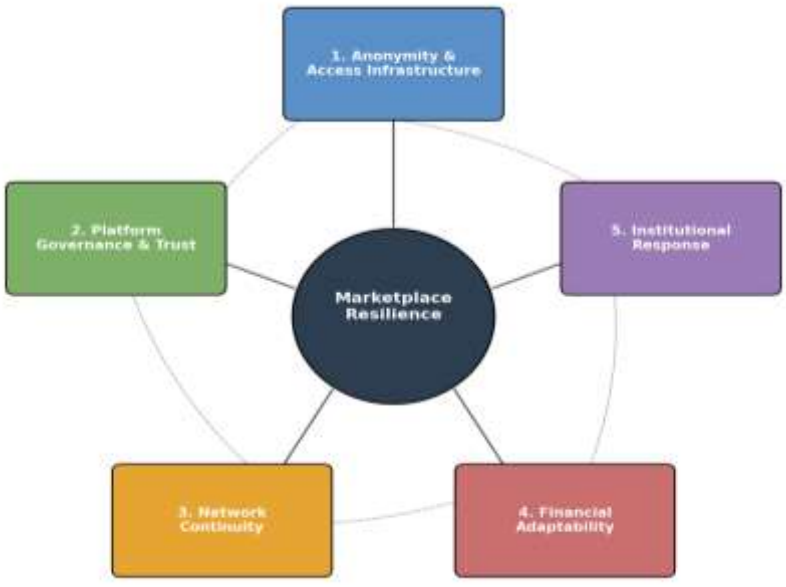

Figure 2. The Five-Layer Dark Web Marketplace Resilience and Disruption Framework.

The institutional response goes beyond takedown efforts to include financial regulation and surveillance with a public-health focus. For instance, during the COVID-19 pandemic, when the need for medical supplies and PPEs has been great, the marketplace has been dominated by illegal listings of medical products and PPEs, which are an opportunity for vendors to exploit institutional gaps in supply-chain oversight, as demonstrated by Bracci et al. (2022). Comparative assessments of enforcement efforts also indicate that financial-intelligence efforts – along

with covert infiltration – provide more enduring and lasting disruption than takedowns targeting only marketplace infrastructure (Bradley, 2019). This evidence highlights the importance of institutional response where such is available, across jurisdictions and embedded in the financial and network level interventions outlined in the previous sections.

4.0. Discussions

The five thematic sections above imply that it is impossible to narrow marketplace resilience down to a single technical capability. The five layers are designed to reduce the technical costs of participation, maintain trust without legal enforcement, enhance the use of network-level multihoming to preserve trading relationships between datacrowns, enable financial innovation in line with the progress of blockchain tracing technologies, and offer external pressure for the other five layers to continuously adapt. Therefore, marketplace resilience is a property of the interaction of all these five layers of the marketplace, and not any one platform, technology or actor.

This multi-layered perspective is also relevant for governance studies specifically because trust mechanisms not only stabilise markets, but can also be used as a tool for law enforcement, as they generate recognisable patterns of behaviour. It is difficult to spoof costly reputation-based trust signals and even more difficult to break, which is why well-established vendors can still win and maintain the trust of their buyers even after losing their marketplaces.

There is also evidence of institutional response which shows that enforcement is not the only answer: There is a place to recover, due to network continuity, in a matter of months, while a major international takedown is helpful in providing intelligence and significant costs for marketplace operators. A case for sustainable disruption: There needs to be coordinated strategy that incorporates technical investigation, intelligence about blockchain, regulatory collaboration and the monitoring of the evolving ecosystems rather than series of single-platform takedowns as isolated events.

From this, this study extends the literature and suggests the Five-Layer Dark Web Marketplace Resilience and Disruption Framework (Figure 2), a cohesive conceptual understanding of marketplace resilience. As opposed to the individual elements of marketplace operations that have been studied elsewhere, the framework depicts resilience as a process of continuous interaction among the anonymity infrastructure, the governance of platforms, continuity of network operations, financial adaptability, and institutional response. One layer can help to temporarily reduce activity in a marketplace, while two layers of simultaneous action is needed to have a lasting effect on activity. The framework is built on recent evidence, provides a coherent conceptual framework, and it also serves as a handy reference for empirical testing, developing policy, and cyber security research.

5.0. Research, Policy and Practice implications

The review has implications that are important to research, policy, and cybersecurity practice. It would be ideal if it helps combat the lack of knowledge regarding the dark web marketplaces by giving a technological, organizational, financial and institutional resilience framework. In methodological terms, it highlights the value of the structured integrative review and thematic synthesis to address cybersecurity problems from a multi-disciplinary perspective,

and the need for an established benchmarking and methodological transparency for future research. The findings are intended to support a change in tack from platform-centred interventions to an 'ecosystem' approach, which requires a cooperation between law enforcement, blockchain analytics, financial regulation and international cooperation, in practice. Future studies are needed to empirically test the proposed framework in various marketplace environments, examine the effects of new technologies like AI and decentralised finance on marketplace resilience, and examine adaptive strategies that can adjust to the fast-changing marketplace dynamics in the illicit economy.

6.0. Conclusion

The central finding is that marketplace resilience is an emergent ecosystem property, meaning that it requires a continuous interaction between all five layers to be created, and thus any intervention that tries to impact a single layer will be continually counterbalanced by the other four, and coordinated multi-layer disruption strategies will be necessary. The Five-Layer Dark Web Marketplace Resilience and Disruption Framework developed in this study is one of the core strengths of this study and provides a conceptual base to understanding each of these mechanisms and how it aids marketplace continuity. The framework brings together the lessons learned from the cyber security, criminology, blockchain analytics, digital platform governance, and financial sector regulations, going beyond the knowledge that can be obtained by looking at individual platforms. It also reveals that coordinated efforts are required to systematically defuse the marketplaces instead of merely marketplaces takedowns, which requires technical investigation, blockchain intelligence, financial control and international collaboration and long-term monitoring.

The review relied on good quality published evidence, but was limited by its requirement to rely on secondary evidence, the dynamic nature of the dark web ecosystem and the challenge in observing anonymous crime. More research is required to test the proposed framework in different marketplace environments, to explore the impact of other new developments on marketplace resilience, such as Artificial Intelligence, Decentralised Finance and Privacy Enhancing Technologies, and to develop longitudinal models to measure adaptation of marketplace ecosystems over time. This will assist in designing more efficient cybersecurity policies, cyber policy regulatory frameworks and more sustainable approaches to disrupting transnational cyber-enabled illicit economies.

Declarations

Source of Funding

This study did not receive grant from any funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare that they have no competing financial interests or person

Consent for Publication

The authors declare that they consented to the publication of this article.

Authors' Contributions

BAB contributed to conceptualization, methodology, investigation, EJA contributed to writing-original draft preparation, IL contributed to writing-review, and editing; SS contributed to supervision, project administration, formal analysis, resources, visualization, investigation; AIW contributed to supervision

Acknowledgements

Authors thank the editorial team of the Asian Journal of Applied Science and Technology for their efforts and the reviewers for their constructive comments.

References

Aldridge, J., & Décary-Hétu, D. (2014). Not an "eBay for drugs": The cryptomarket Silk Road as a paradigm shifting criminal innovation. Social Science Research Network. https://doi.org/10.2139/ssrn.2436643.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. International Journal of Drug Policy, 35: 7–15. https://doi.org/10.1016/j.drugpo.2016.04.020.

Bracci, A., Nadini, M., Aliapoulios, M., McCoy, D., Gray, I., Teytelboym, A., Gallo, A., & Baronchelli, A. (2022). Vaccines and more: The response of Darkweb marketplaces to the ongoing COVID-19 pandemic. PLoS ONE, 17(11): e0275288. https://doi.org/10.1371/journal.pone.0275288.

Bradley, C. (2019). On the resilience of the dark net market ecosystem to law enforcement intervention [Doctoral thesis, University College London]. UCL Discovery. https://discovery.ucl.ac.uk/id/eprint/10080409/.

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd International Conference on World Wide Web, Pages 213–224, Association for Computing Machinery. https://doi.org/10.1145/2488388.2488408.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime, Law and Social Change, 67(1): 55–75. https://doi.org/10.1007/s10611-016-9644-4.

dos Reis, E.F., Teytelboym, A., ElBahrawy, A., De Loizaga, I., & Baronchelli, A. (2024). Identifying key players in dark web marketplaces through Bitcoin transaction networks. Scientific Reports, 14(1): 2385. https://doi.org/10.1038/s41598-023-50409-5.

Duxbury, S.W., & Haynie, D.L. (2018). Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. Social Networks, 52: 238–250. https://doi.org/10.1016/j.socnet.2017.09.003.

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. Scientific Reports, 10(1): 18827. https://doi.org/10.1038/s41598-020-74416-y.

Europol (2017). Internet Organised Crime Threat Assessment (IOCTA) 2017. Europol. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2017.

Europol (2026). Internet Organised Crime Threat Assessment (IOCTA) 2026. Europol.

Financial Action Task Force (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF. https://www.fatf-gafi.org.

Financial Action Task Force (2026). Virtual assets: Targeted update on implementation of the FATF standards. FATF.

Ladegaard, I. (2019). Crime displacement in digital drug markets. International Journal of Drug Policy, 63: 113–121. https://doi.org/10.1016/j.drugpo.2018.09.013.

Nadini, M., Alessandretti, L., Di Giacinto, F., Baronchelli, A., & Vespignani, A. (2022). Emergence and structure of online illicit trade networks. Nature Human Behaviour, 6(4): 558–566. https://doi.org/10.1038/s41562-021-01259-0.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

Scharnowski, S. (2024). Dark web traffic, privacy coins, and cryptocurrency trading activity. Finance Research Letters, 67: 105875. https://doi.org/10.1016/j.frl.2024.105875.

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox: Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. International Journal of Drug Policy, 35: 58–68. https://doi.org/10.1016/j.drugpo.2015.12.010.